AN INTRODUCTION TO THE LIGHTNING NETWORK

⚡ BY STACIE WALEYKO & DESIREE DICKERSON

JULY 30, 2019

DESIREE DICKERSON

LIGHTNING LABS

- Head of Operations @Lightning Labs
- Bitcoin by way of r/Dogecoin
- Former management consultant
- UChicago + Georgetown

STACIE WALEYKO

CASA

- Backend engineer @CasaHODL
- Enterprise blockchain runaway
- Previously developing for ad tech
- BSc Comp Science & Math - URI

WHAT IS LIGHTNING?

WHAT DOES IT HAVE TO DO WITH BITCOIN?

WHY BITCOIN WHEN WE HAVE OTHER PAYMENT SYSTEMS?

OPEN

Anyone can join or leave the network.

CENSORSHIP RESISTANT

Especially important for political dissidents & those that don't enjoy the same kinds of financial freedoms that others have.

NO THIRD PARTIES REQUIRED

Digitally transfer value without the need of an intermediary.

FAST

At best, Bitcoin does roughly 7 transactions a second

CHEAP

Fees are unreliable and constantly fluctuating

SCALABLE

Small payments can flow through the network similar to how packets flow through the Internet

BONUS: INCREASED PRIVACY

Not all transactions need to be on the blockchain

LIGHTNING IS A **PROTOCOL** THAT MAKES BLOCKCHAINS **FAST & SCALABLE**

HOW DOES IT WORK?

THE LN PROTOCOL

THREE LN IMPLEMENTATIONS

Lightning Labs - lnd

Blockstream - clightning

ACINQ - eclair

USING INTEROPERABLE STANDARDS

BOLT

WHO ARE THE PARTICIPANTS?

Businesses, research groups, and everyday people

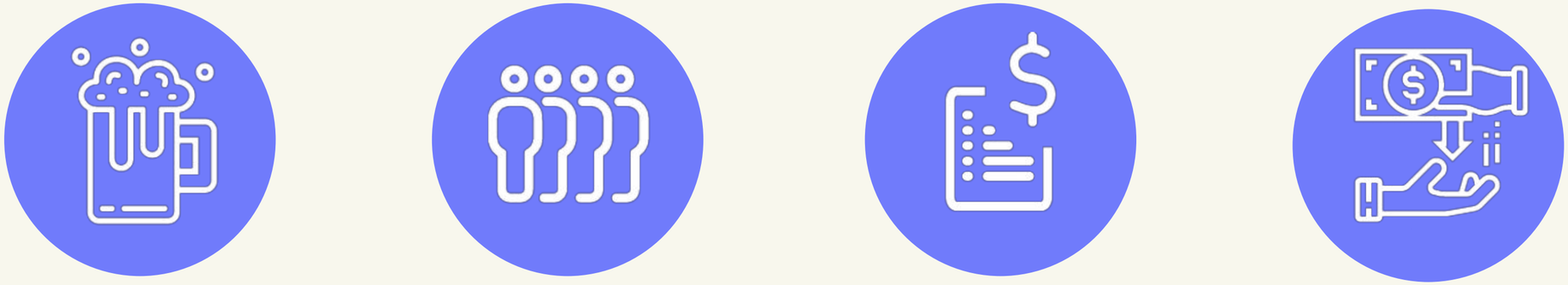
PAYMENT CHANNELS

- Direct connections between two participants
- Bi directional
- Each time you want to spend, you sign a transaction and give it to the other party, like a receipt

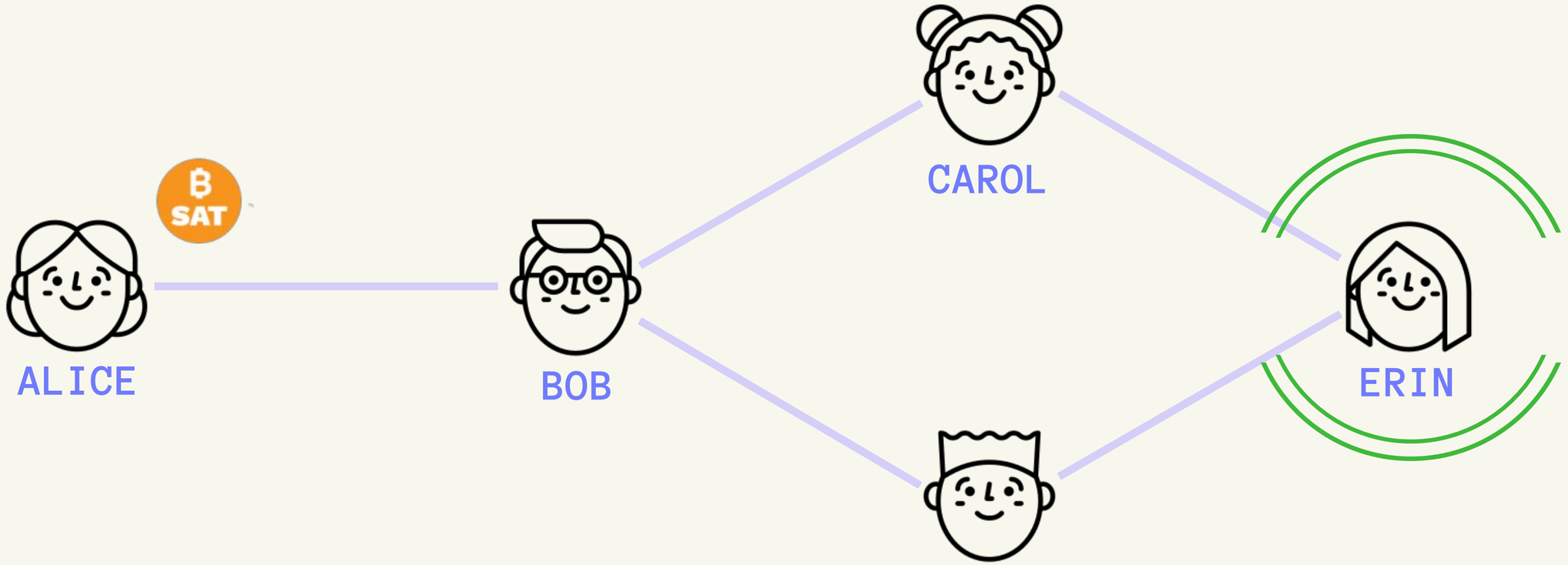
UNDER THE HOOD

- **Anchored to the underlying blockchain -** 2-of-2 multi sig transaction (tx).
- **Lightning fast! -** Initial (opening) tx is limited by the blockchain, but afterwards participants **can transact instantly** with the funds in the channel.
- **Batch settling off chain transactions** - For the price of one opening tx, and one closing tx, the LN channel can be used to transact as many times as needed.
- **"local consensus"** while the channel is open, and **"global consensus"** when it closes.

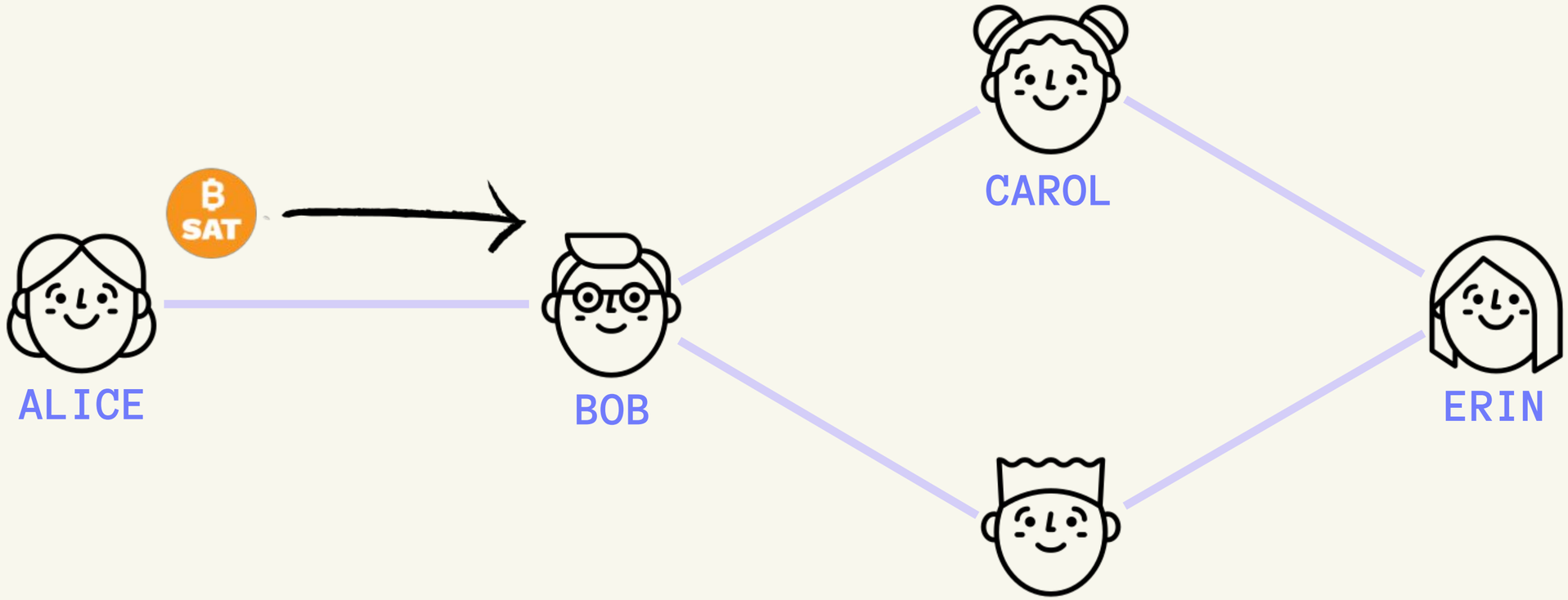
THE BAR EXAMPLE



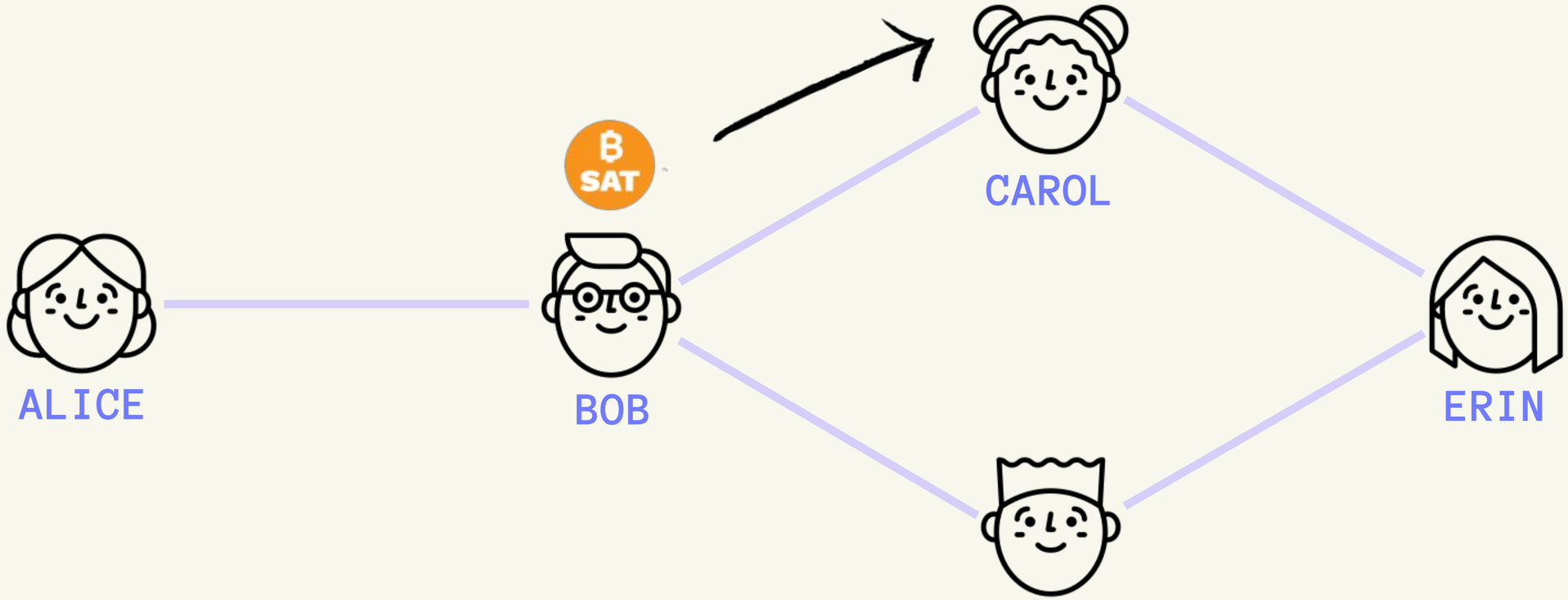
A ROUTING EXAMPLE



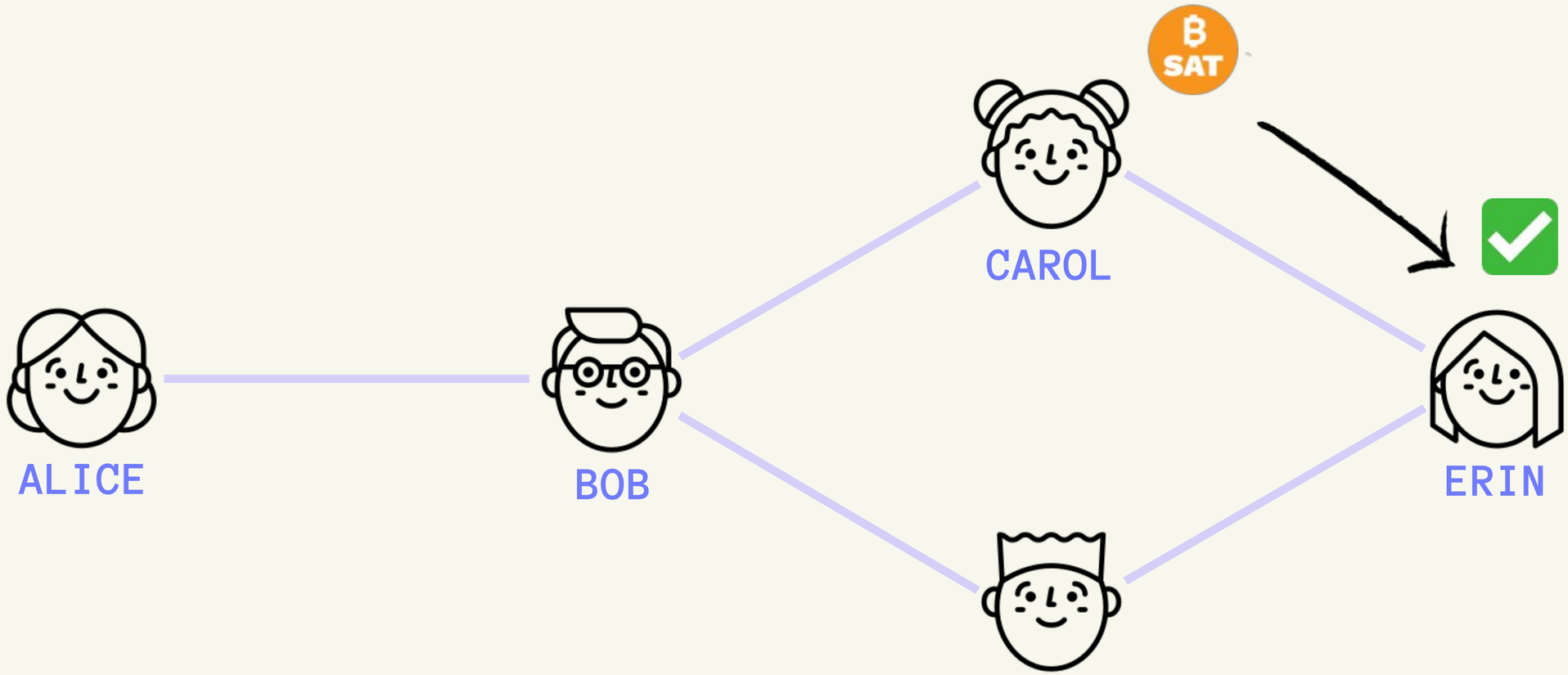
A ROUTING EXAMPLE



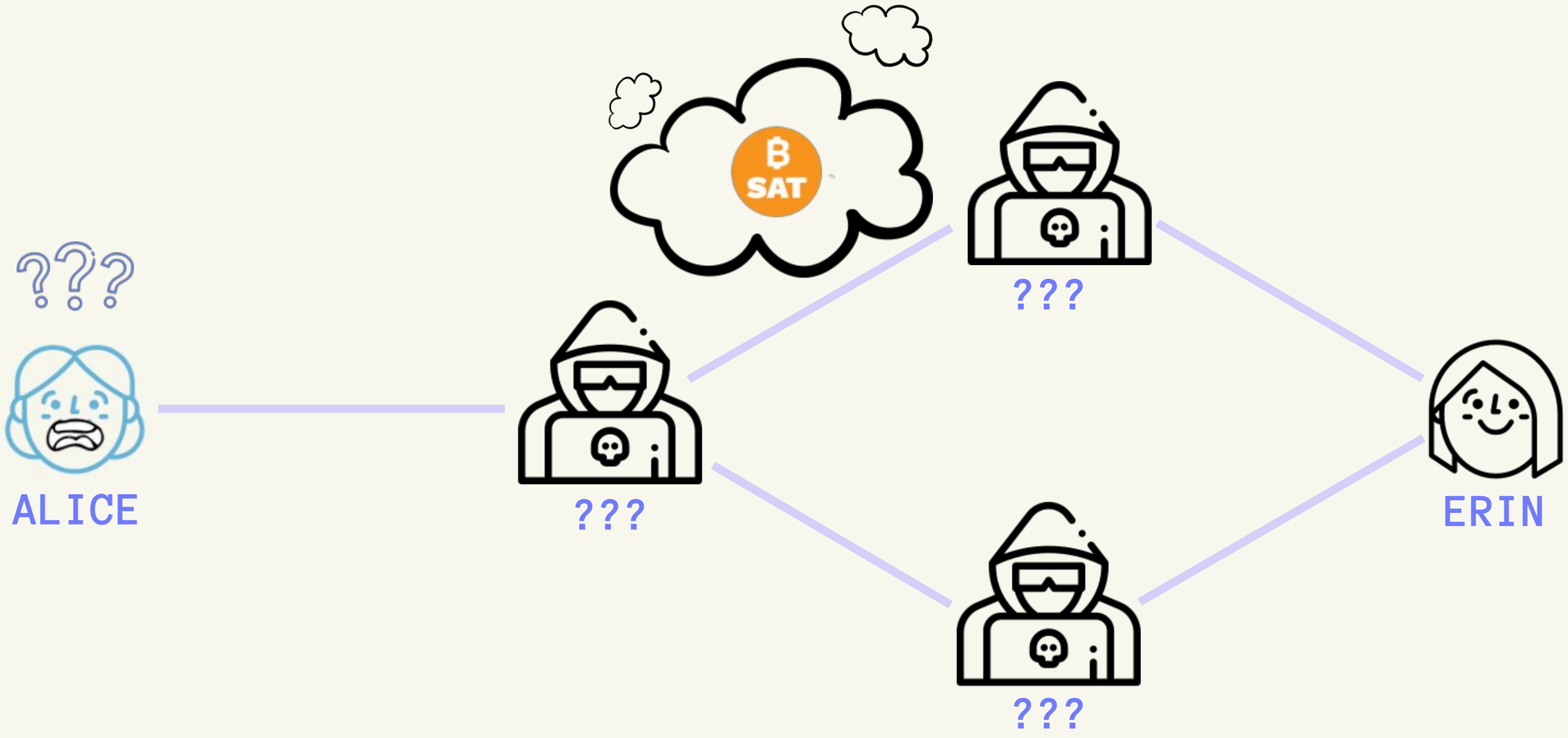
A ROUTING EXAMPLE



A ROUTING EXAMPLE



WHAT ABOUT TRUST?



TECHNICAL DETAILS: HTLCS

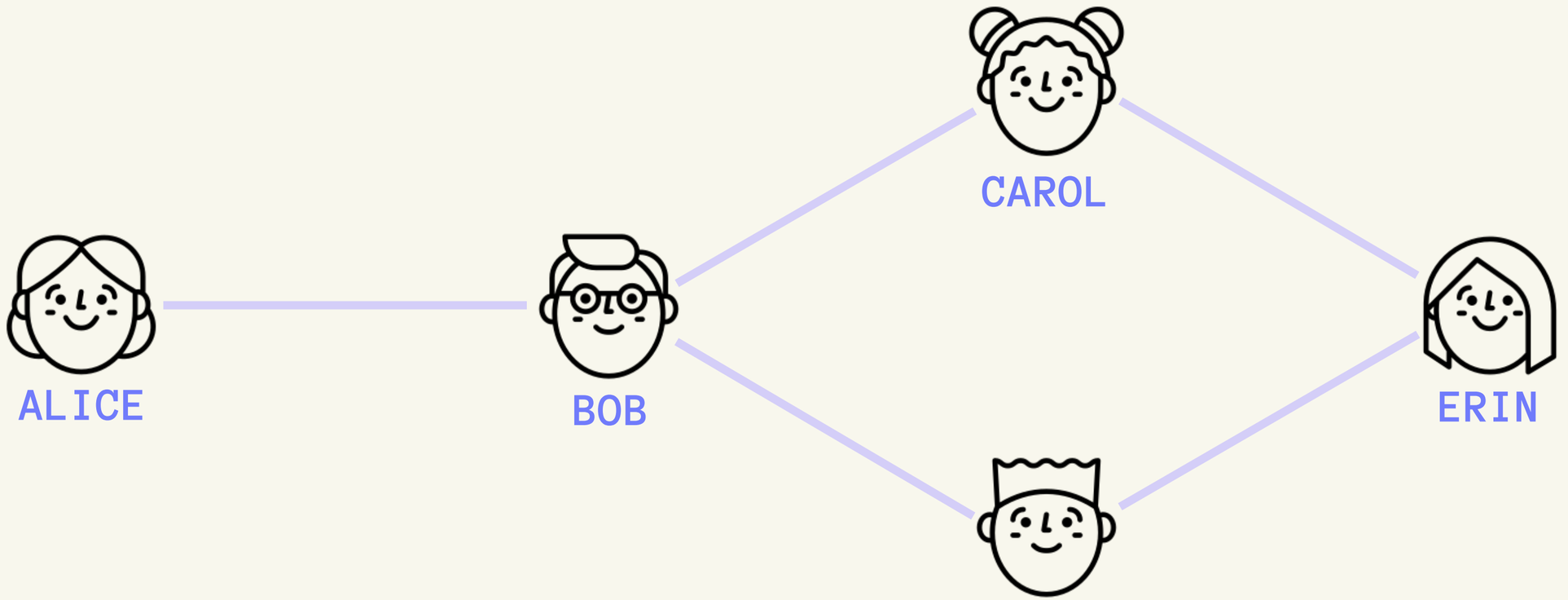
HASH TIME LOCKED CONTRACTS

A class of payments that involve

- **Hashlocks**: Funds are only sent upon proof of outgoing payment. Each receiver must generate a cryptographic proof of payment.

- **Timelocks**: If any participant does not receive a payment, the entire transaction times out and all parties are refunded.

-> CANNOT STEAL FUNDS


CAROL
ALICE
BOB
ERIN

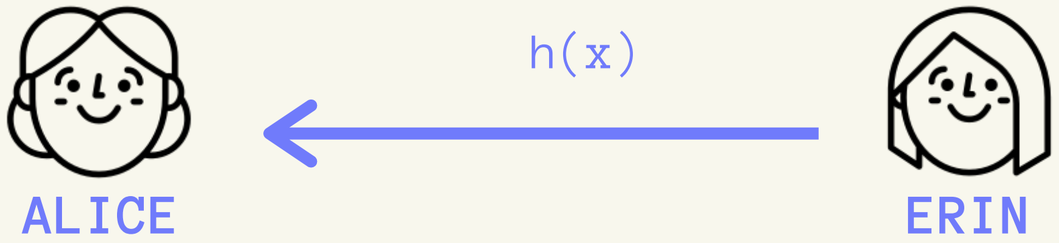
ALICE WANTS TO PAY ERIN 100 SATOSHIS (SATS)

ERIN

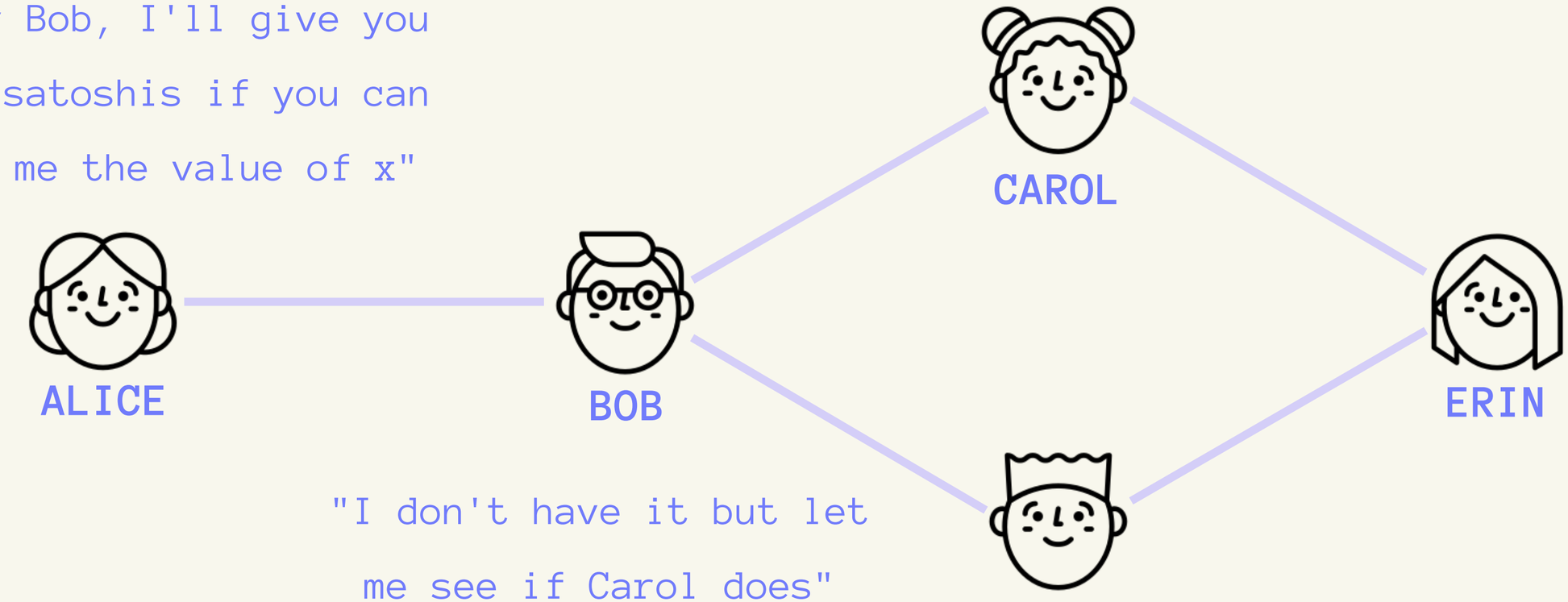
x = a random number

h(x) = the hash of x

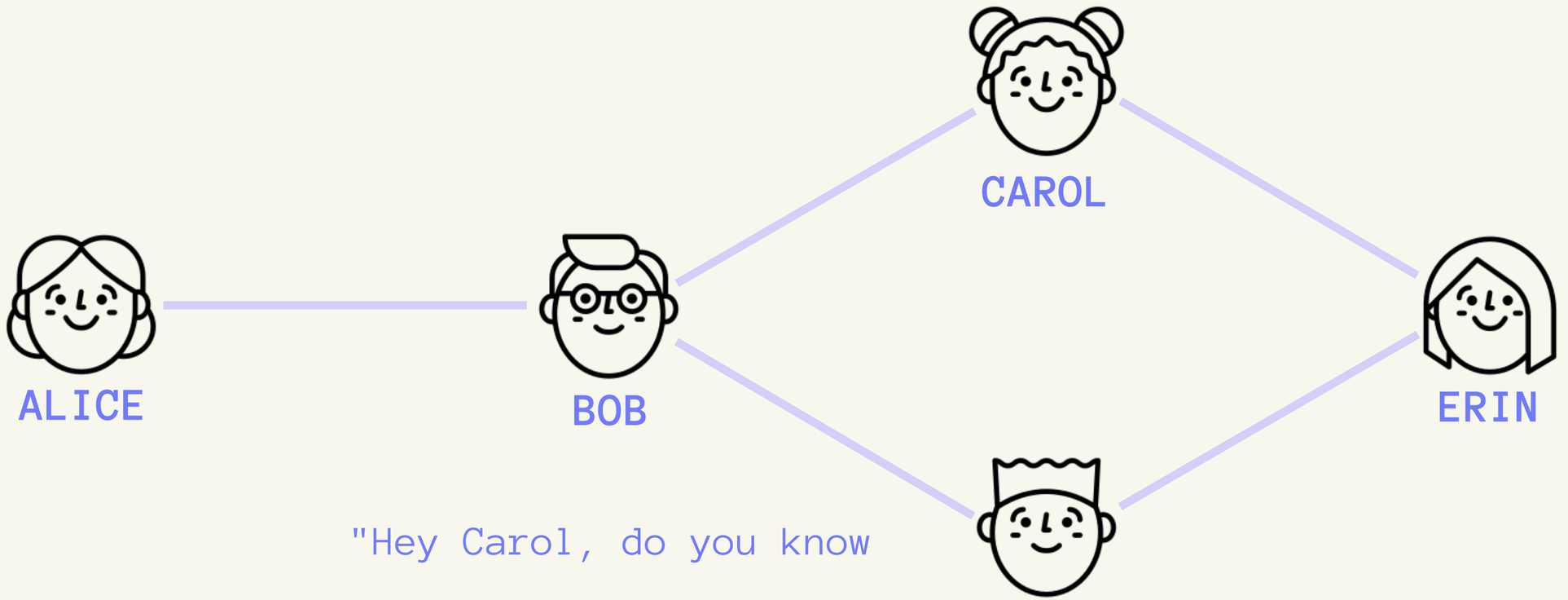
INVOICE STEP: ERIN GIVES THE HASH TO ALICE

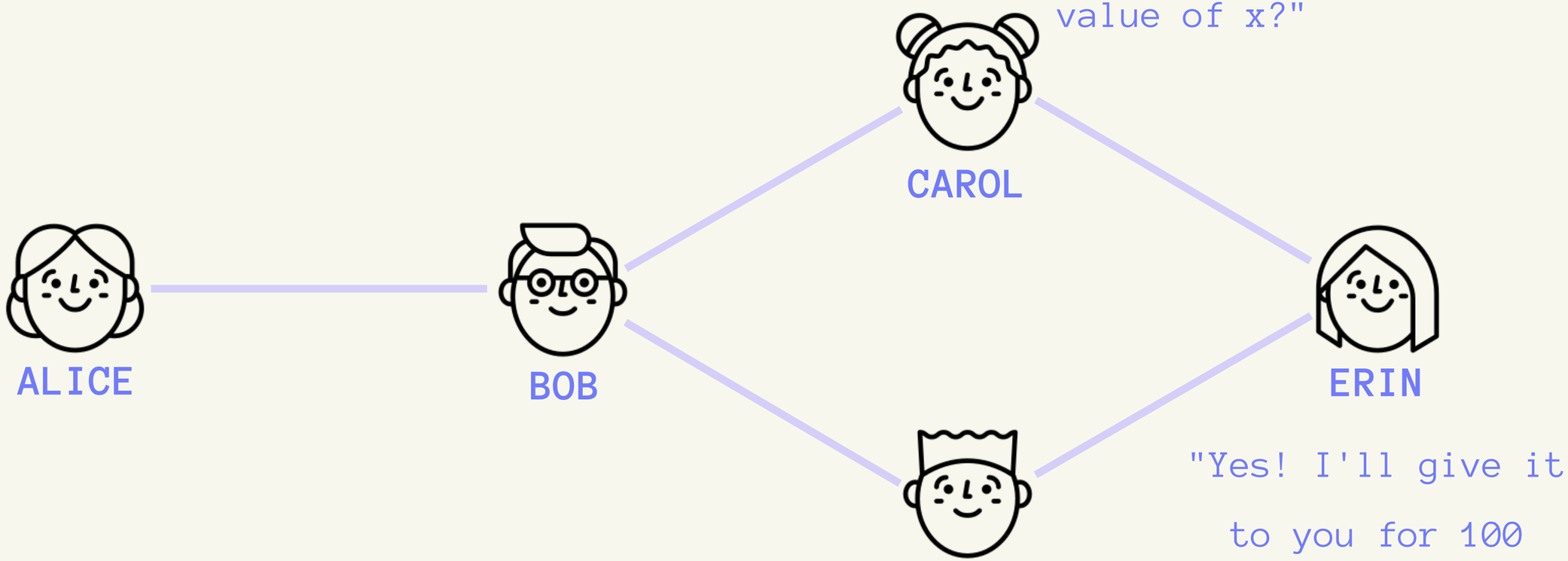


"Hey Bob, I'll give you 100 satoshis if you can get me the value of x"



"I don't have it but let me see if Carol does"


"No, but Erin might"
CAROL
ALICE
BOB
ERIN
"Hey Carol, do you know the value of x? I'll give you 100 sats"

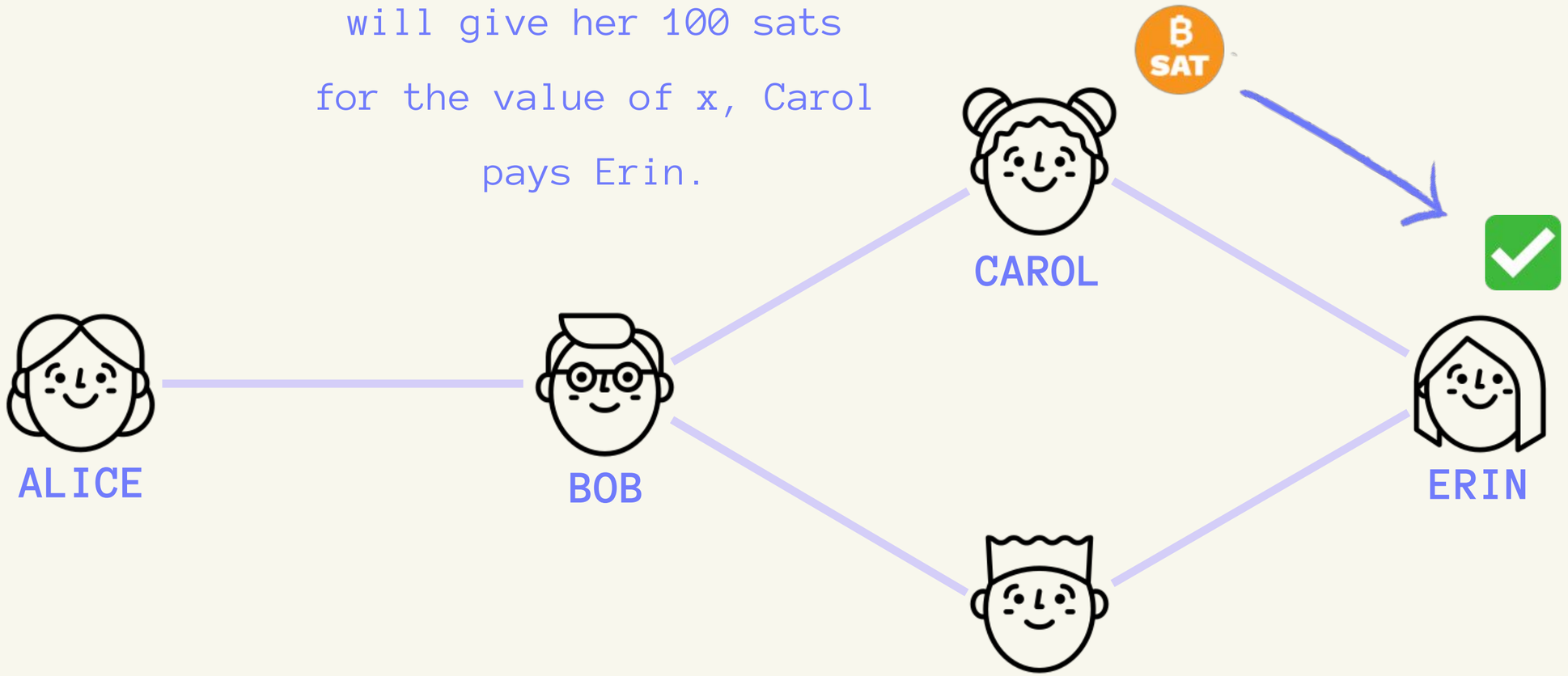

"Erin, do YOU know the value of x?"
CAROL
ALICE
BOB
ERIN
"Yes! I'll give it to you for 100 satoshis"

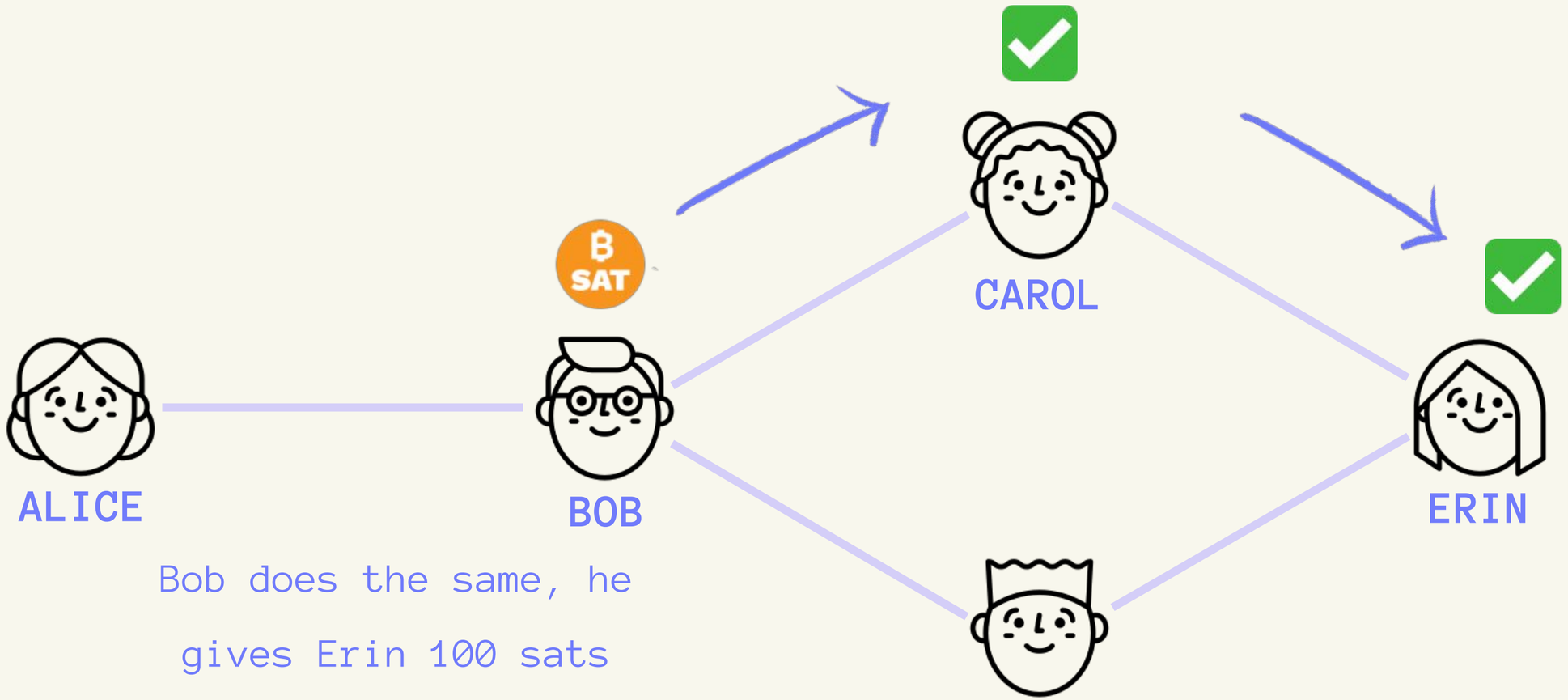
Because Carol knows Bob

will give her 100 sats

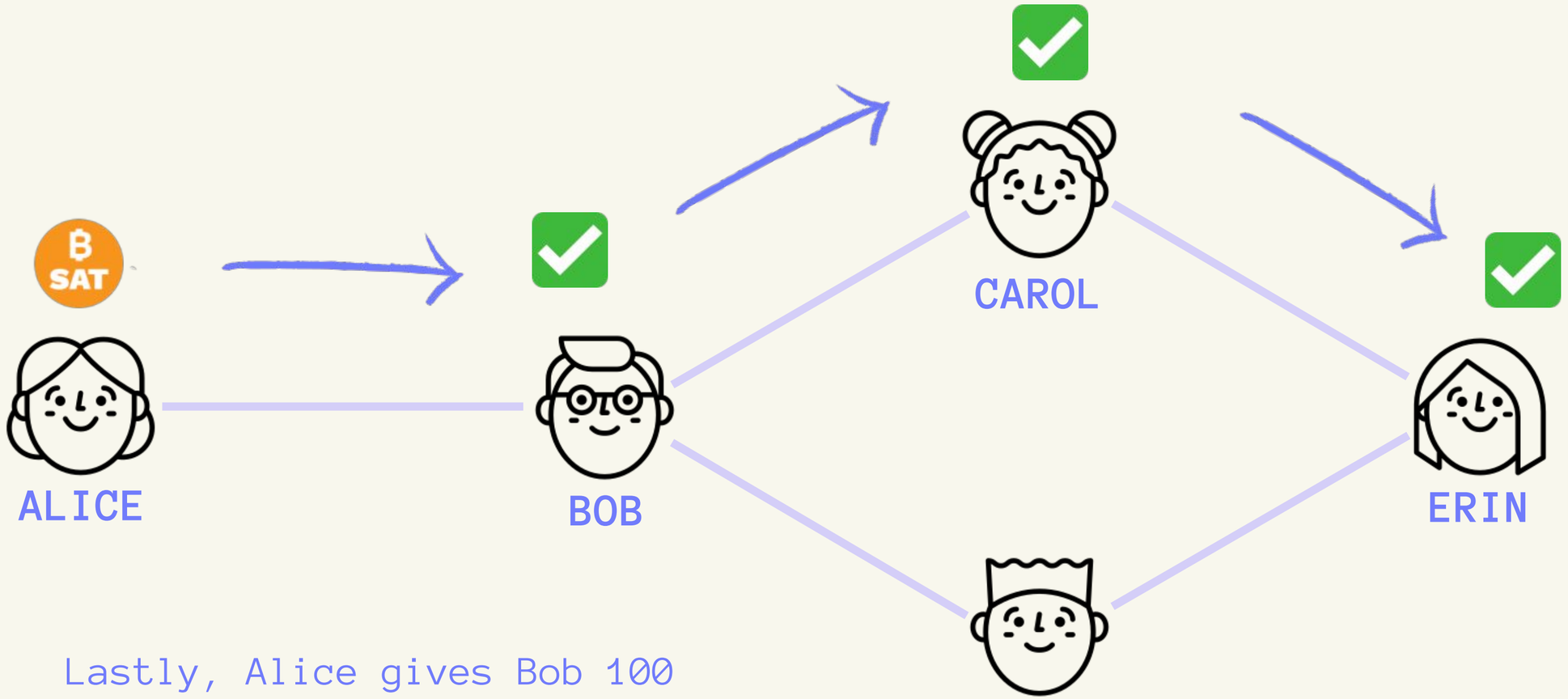
for the value of x, Carol

pays Erin.





Bob does the same, he gives Erin 100 sats because he knows Alice will give him 100 sats for the value of x.



Lastly, Alice gives Bob 100 sats for the value of x

TECHNICAL DETAILS

ONION STYLE ROUTING

Don't know where the payment originated, or what its final destination is

PENALTY FOR ATTEMPTING TO CHEAT

Broadcasting an old channel state results in the forfeiture of all funds

BEYOND BITCOIN

Cross chain atomic swaps: Lightning can work on other blockchains, thus enabling the transfer of different types of assets.

HOW CAN I JOIN IN ON THE FUN?

RUN A NODE

Build your own (Raspibolt w LND is popular, Pierre Rochard's Node Launcher), buy one (Casa)

USE NEUTRINO

Lightning Labs + Desktop or Mobile App

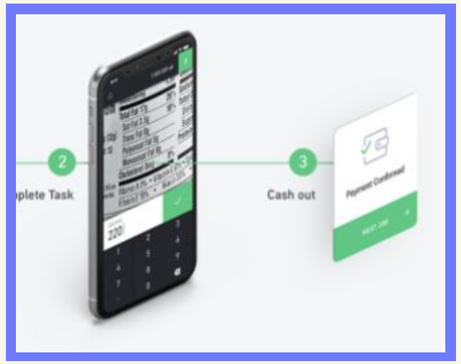
USE A CUSTODIAL WALLET

Bluewallet, Wallet of Satoshi, Breez, etc.

WALLET DEMO

PLAY GAMES

BUY PIZZA



EARN

SATOSHIS!

WAYS YOU CAN USE LIGHTNING TODAY

DEMO!

IMPROVING THE STATUS QUO + CREATING NEW MARKETS

TRADITIONAL

- Decentralized exchanges
- High frequency trading
- Paywalls
- AdTech

NEW MARKETS

- Streaming
- Content seeding
- Gaming
- Gig economy
- P2P bandwidth and hosting
- TBD!

OUTSTANDING CHALLENGES

MORE DEVELOPMENT

The technology is still in nascent stages and needs more development and testing.

NETWORK ADOPTION

Lack of liquidity and nodes make it difficult to use. Routing errors are common.

EDUCATION

Onboarding and ongoing usability are challenges beginning with bitcoin. Lightning is an additional hurdle.

WHAT'S NEXT - NEW DEVELOPMENTS

WATCHTOWERS

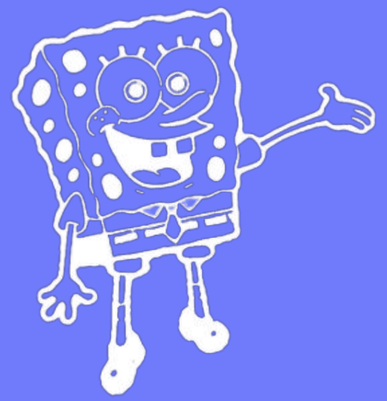
Protect your channels from malicious activity

AMP

Lightning Labs + Desktop or Mobile App

WUMBO!

#craefulgang -> the limit does not exist!



JOIN US!

BECOME ONE OF US!

Casa

- Frontend Engineer

Lightning Labs

- Frontend App Developer
- Cryptographic Protocol Engineer
- Lightning Infrastructure Engineer
- DevOps Engineer
- Technical Product Manager

JOIN THE COMMUNITY

- Casa Node & SatsApp Telegrams
- LND Dev Slack
- Lightning Makers Telegram
- Events:
  - The Lightning Conference
    - October 19-20 | Berlin
  - Crypto Springs
    - September 23-25 | Palm Springs

@STACIEWALEYKO

@CASAHODL

@DICKERSON_DES

@LIGHTNING

THANK YOU!